Office of the Information and
Privacy Commissioner of Alberta

**PERSONAL INFORMATION PROTECTION ACT**
**Breach Notification Decision**

| | |
|---|---|
| **Organization providing notice under section 34.1 of PIPA** | Nissan Canada Finance (Organization) |
| **Decision number (file number)** | P2018-ND-114 (File #007362) |
| **Date notice received by OIPC** | December 20, 2017 |
| **Date Organization last provided information** | June 6, 2018 |
| **Date of decision** | August 13, 2018 |
| **Summary of decision** | There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA). |
| **JURISDICTION** | |
| **Section 1(1)(i) of PIPA "organization"** | The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved all or some of the following information:<br><br>• name,<br>• address,<br>• vehicle make and model,<br>• vehicle identification number (VIN),<br>• credit score,<br>• loan amount, and<br>• monthly payment.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On December 11, 2017, the Organization received an extortion demand from an unknown person(s) claiming to have gained access to the personal information of the Organization's customers.<br>• The Organization investigated and discovered there was an unauthorized access to certain of its servers that held personal information of Canadian customers who financed their vehicles with the Organization.<br>• The Organization also determined no payment card information was affected.<br>• The Organization determined that there is no indication of any external breach of its systems with respect to this incident which is being assessed as emanating from inside the Organization. |
| **Affected individuals** | The Organization reported it does not know the exact number of affected individuals, but has sent letters to approximately 932,000 people. |
| **Steps taken to reduce risk of harm to individuals** | • Investigated the incident.<br>• Notified all customers in the impacted database, including those not obviously affected.<br>• Offered free credit monitoring to all customers.<br>• Established a call centre to answer questions from affected individuals.<br>• Reported the incident to Canadian privacy regulators and law enforcement. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on January 30, 2018 and February 28, 2018. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects. | The Organization did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated that it is offering "12 months of credit monitoring services …at no cost." The Organization recommended to its customers to "review your bank account and payment card statements carefully and call your bank it you see any suspicious transaction… you should also report the possible threat to your identity to local law enforcement, the Canadian Anti-Fraud Centre, or the federal or provincial privacy commissioners…".<br><br>In my view, a reasonable person would consider that the contact and profile information (relationship to the Organization), along with the limited financial information, could be used to cause the significant harms of identity theft, fraud and/or financial loss. |

| | |
|---|---|
| **Real Risk**<br>The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm. | The Organization did not specifically assess the likelihood that significant harm would result from this incident.<br><br>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and ransom demand). Further, it is unclear how long the information may have been exposed before the breach was discovered by the Organization. |

**DECISION UNDER SECTION 37.1(1) OF PIPA**

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the contact and profile information (relationship to the Organization), along with the limited financial information, could be used to cause the significant harms of identity theft, fraud and/or financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and ransom demand). Further, it is unclear how long the information may have been exposed before the breach was discovered by the Organization.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in letters sent January 30, 2018 and February 28, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner